REMARKS

Claims 1-15, 17-62, 64-80, and 82-88 are pending in this application. All of the claims have been rejected. In view of the following remarks, Applicants respectfully request reconsideration of the Application.

Rejections Under 35 USC §103(a)

In paragraph 3 of the Office Action, the Examiner rejected claims 1-5, 10-15, 17-25, 28-62, 64-80, and 82-88 under 35 U.S.C. §103(a) over Leporini et al. (U.S. Pub. No. 2003/0182579, hereinafter *Leporini*) in view of Pensak et al. (U.S. Pub. No. 2002/0029340, hereinafter *Pensak*).

The Examiner contends that *Leporini* teaches "a method for providing access control management to electronic data, the method comprising establishing a secured link with a client machine when an authentication request is received from the client machine, the authentication request including an identifier identifying a user of the client machine to access the electronic data, wherein the electronic data is secured in a format including security information and an encrypted data portion, the security information including file key and access rules and controlling restrictive access to the encrypted data portion authenticating the user according to the identifier (see paragraphs 0003, 0004, 0008, 0015, 0024, 0027, 0036, 0041-0046, 0052, 0203, 00437)." Applicants traverse.

Applicants note, with respect to the previously submitted arguments as to why *Leporini* does not provide support for elements of claims, that the Examiner has not provided any feedback or counter-arguments other than the "applicant's arguments with respect to claims 1-15, 17-62, 64-80, and 82-88 have been considered but are moot in view of the new ground(s) of rejection." However, the new grounds of rejection involve the same reference (i.e., *Leporini*) for

support of the same elements of the claims. As such, Applicants' reiterate portions of their previously present arguments with respect to *Leporini* and respectfully request that the Examiner provide a detailed response.

Independent claim 1 requires "establishing a secured link between a server providing the access control management and a client machine when an authentication request is received from the client machine." This requirement further necessitates the existence of "a client machine" and "a server providing the access control management." Moreover, the requirement necessitates a step of "establishing a secured link" between the server and the client machine "when an authentication request is received from the client machine."

Applicants propose that "a client machine" in *Leporini* is the HDVR. While there are many components discussed in the reference that potentially could be considered a client machine, *Leporini* specifically identifies the HDVR as a client in paragraph [0251], and Applicants view a hard disk video recorder as a machine. If the Examiner views some component other than the HDVR as the client machine, Applicants request that the Examiner explicitly identify the component and indicate the support in *Leporini* for considering said component to be the client.

Applicants propose that "a server providing the access control management" is the CMPS server specifically referred to in paragraphs [0267], [0284], and [0330]. Here, too, there are a number of servers provided in *Leporini*, but *Leporini* notes that "navigation and usage constraint information [is] associated with the CMPS server" (paragraph [0267]). The "navigation and usage constraint information" would appear to provide "access control management" in *Leporini*. Again, if the Examiner views a different server as responsible for providing the access control management in *Leporini*, the

Examiner is encouraged to explicitly provide and justify the alternative interpretation.

As noted above, the limitation of claim 1 being discussed requires "establishing a secured link" between the server and the client machine "when an authentication request is received from the client machine." Thus, claim 1 requires that the secured link is established when an authentication request is received from the client machine. Although Applicants note in *Leporini* instances of secured links, connections, channels, and interfaces (e.g. [0296] [0309] [0317] [0329] [0347] [0355] [0360] [0364] [0380] [0404] [0410] [0423] [0436] [0437] [0439] [0443] [0444] and [0460]), none of these instances pertain to a link that is established between the HDVR and the CMPS server when the HDVR requests authentication.

For example, the references to secured connections found in paragraphs [0296], [0309], and [0317] do not involve the HDVR. These paragraphs pertain to the embodiments illustrated in FIGs. 24-26. In each instance, the secure connection is associated with either stage 407, 503, or 607. In each embodiment, the implicated stage is between the CMPS and the RCARD_device, and not the HDVR.

The references to secured connections identified in paragraphs [0329] - [0423] pertain to connections between SM CMPS and SM CAS (stage 1500 in FIG. 30, stages 1600 and 1612 in FIG. 32, and stage 1700 in FIG. 34). The communications between these two security modules (SM) take place within the decoder/receiver 13 (FIG. 2) and do not involve the HDVR (e.g. mass storage device 370 (FIG. 2). As evidence, *Leporini* notes that "[t]he receiver/decoder itself comprises a daughter conditional access smartcard 48" (paragraph [0198], see FIG. 2) and "[t]he receiver/decoder portion of the CMPS 300 comprises a security module (in the form of a removable smartcard) 320 (not shown)" (paragraph

[0199], see FIG. 2). The conditional access smartcard 48 is identified with the CAS SM in paragraph [0339].

Paragraph [0437] was particularly noted by the Examiner. This paragraph pertains to "APIs which may be included in the security library of the CMPS" and that are described in subsequent paragraphs, such as noted paragraphs [0439] – [0460]. These APIs "raise issues on the usage of a client-server model between the CMPS SM and the group of equipment with which a secure connection (SAC) is established" (paragraph [0437]). Nowhere in these paragraphs is the HDVR implicated as a device with which the CMPS SM creates a secure connection.

Even if, *arguendo*, paragraphs [0437] – [0460] can be read to implicate that a secure connection is created between the CMPS SM and the HDVR, such a connection is to the CMPS SM (i.e., a smartcard) and not to the CMPS server identified above as the server of claim 1 that provides access control management. Moreover, there is no indication that such a secure connection is established "when an authentication request is received" from the HDVR.

Turning next to the requirement of claim 1 that "the authentication request include[s] an identifier identifying a user of the client machine to access the electronic data." Applicants note that *Leporini* teaches that "[a]t the instigation of the HDVR sub-system, a session is opened with CMPS allowing the recovery of the CMM data at the time of each event" (paragraph [0265]) and "[a]t the time of arrival of this event, HDVR requests the CMM to obtain navigation and usage constraint information associated with the CMPS server" (paragraph [0267]). Although the HDVR makes a request, Applicants assert that the request does not constitute an authentication request because the request does not seek to authenticate. Rather, the request is for information, specifically navigation and usage constraint information.

Even if, *arguendo*, it is assumed that a request for navigation and usage constraint information is a request for authentication, Applicants further note that *Leporini* does not teach that the request includes an identifier identifying the user of the HDVR.

Claim 1 further requires "authenticating the user according to the identifier." Applicants recognize that, according to *Leporini* "[i]n the personalisation mode the CMPS system is responsible for the creation of personalised copies by encrypting the CMM by a unique user key. This key moreover depends on a content identifier (content_id) serving to broaden the user key. All usage of recorded content requires a security module to be present to personalise the copy" (paragraph [0378]). As noted above, claim 1 requires that the identifier identify the user, yet in the personalization mode of *Leporini*, the unique "user" key depends on a content identifier. Thus, it actually identifies the content, rather than actually identifying the user. Even if the unique user key is viewed as an identifier that identifies the user, the user key is not used to authenticate the user in *Leporini*.

It is also noted that the electronic data in claim 1 is "in a format including security information and an encrypted data portion, the security information including a file key and access rules." For example, a header of a secured document may include encrypted security information including access rules to control access to an encrypted data portion of the secured document (*Application*, paragraph [0011]). As such, the content that the user is attempting to access contains the security information including the access rules.

If one were to assume that the usage rules of *Leporini* are equivalent to the access rules of claim 1, which Applicants disagree with, these usage rules are not embodied within the content. The "usage rules are encapsulated in Usage Rules Messages ("URM")" (paragraph [0203]). "URMs may be obtained prior to the

broadcasting or recording of programmes" (paragraph [00205]), and "it is important to note that the URMs may be sent independently of the content" (paragraph [0207]). As such *Leporini* is further lacking this element of claim 1.

Lastly, claim 1 requires "activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules." The Examiner notes that *Leporini* does not teach this limitation and contends it can be found in *Pensak*.

As previously noted, the access rules are in the security information which are a part of the electronic data the user is attempting to access. In contrast, *Pensak* provides a "remote server [which] stores a unique identifier for the information and associates an encryption/decryption pair and access policies with the information... Software components residing on the viewing user's computer retrieve the associated decryption key and policies" (see *Abstract*). As such, the access policies of *Pensak* are stored, not with the information being accessed, but at a remote server. Therefore, *Pensak* cannot disclose use of a user key to "access the access rules in the security information" of the electronic data since the access rules in *Pensak* are not located with the security information of the electronic data.

Moreover, even if, *arguendo*, *Leporini* does teach "activating a user key after the user is authenticated, wherein the user key is used to access the access rules in the security information, the file key can be retrieved to decrypt the encrypted data portion only if access privilege of the user is successfully measured by the access rules." Applicants assert that one of ordinary skill in the art at the time the invention was made would not have been motivated to

combine *Leporini* with *Pensak*. The Examiner states that the motivation to combine the references is that the modification "would have ensured the information transmitted, received and/or stored by the system remains secure against unauthorized use and unlawful access."

However, Applicants fail to see where one of ordinary skill in the art at the time the invention was made would have been motivated to look to *Pensak* or any other reference, to secure information against unauthorized use and unlawful access when *Leporini* already encrypts the content management information and the conditional access information for security purposes and proposes that the "content management information may be encrypted using a different exploitation key from that used to encrypt the conditional access information, and may be encrypted using a different encryption algorithm" for still greater security (paragraph [0024]).

Furthermore, *Leporini* appears to be an inappropriate reference to be used both against the present claims and in association with *Pensak*. *Leporini* pertains to digital television and the broadcast of programs to users. In contrast, *Pensak* is concerned with encrypting and protecting text documents (paragraph [0015]), while embodiments of the present invention are directed to providing security to digital assets including, but not limited to, documents, multimedia files, data, executable codes, images, and texts. As such, it is arguable that one skilled in the art would not find *Leporini* relevant art with respect to the present Application or to *Pensak*, and would not be motivated to combine *Leporini* with *Pensak* to obtain the elements of claim 1.

Based at least upon the above remarks, Applicants submit that claim 1 is allowable in view of the combination of *Leporini* and *Pensak* and request that claim 1 be allowed. Furthermore, since claims 2-15, and 17-19 depend from claim

1, Applicants submit that claim 2-15, and 17-19 are also allowable for at least the same reasons given above in conjunction with claim 1.

In paragraph 18, the Examiner rejected claim 20 alleging that *Leporini* teaches "a method for providing access control management to electronic data in a client machine, the method comprising authenticating a user attempting to access the electronic data; maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, includes a header and an encrypted data portion, the header further includes security information controlling who, how, when and where the secured electronic data can be accessed and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme." Applicants traverse.

Claim 20 requires "authenticating a user attempting to access the electronic data." While *Leporini* teaches an "encryption key [] associated with a device, subscriber, commercial offer, or content" (paragraph [0037]), *Leporini* does not specifically teach a process of authenticating a subscriber who is attempting to access the electronic data. And as noted above with respect to claim 1, even if the unique user key of *Leporini* is viewed as an identifier that identifies the user, the user key is not used to authenticate the user.

Claim 20 further requires "maintaining a private key and a public key, both associated with the user, wherein the electronic data, when secured, ***includes a header and an encrypted data portion, the header further includes security information controlling who, how, when or where the secured electronic data can be accessed*** and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme" (emphasis added). *Leporini* does not teach both public and private keys associated with a

user. *Leporini* does provide general and local exploitation keys (paragraph [0240]), but these keys do not constitute public and private keys associated with the user. Additionally, *Leporini* does not teach electronic data having a header wherein "the header further includes security information controlling who, how, when or where the secured electronic data can be accessed."

Moreover, one of ordinary skill in the art at the time the invention was made would not have been motivated to combine *Leporini* with *Pensak* for the same reasons provided above with respect to claim 1.

Based upon at least the above remarks, Applicants submit that claim 20 is allowable in view of the combination of *Leporini* with *Pensak*, and request that claim 20 be allowed. Furthermore, since claims 21-30 depend from claim 20, Applicants submit that claim 21-30 are also allowable for at least the same reasons given above in conjunction with claim 20.

Regarding independent claim 31, the Examiner contends in paragraph 27 that *Leporini* teaches "a method for providing access control management to electronic data, the method comprising receiving a request to access the electronic data; determining security nature of the electronic data; when the security nature indicates that the electronic data is secured, the electronic data including a header and an encrypted data portion, the header including security information controlling restrictive access to the encrypted data portion and the encrypted data portion is an encrypted version of the electronic data according to a predetermined cipher scheme." Applicants traverse.

Claim 31 requires "determining [the] security nature of the electronic data by intercepting the electronic data moving from the store through an operating system layer to an application for the data." *Leporini* teaches, with respect to playback of recorded programs with the HDVR, that "[a]t the time of using a

recorded content, the CMPS ensures the validity of the associated rights by comparing the usage rules presented in the recorded CMM with the rights acquired by the subscriber and included in the security module (SM)" (paragraph [0279]). Clearly, the security nature of the content of *Leporini* is determined by comparing the usage rules presented in the recorded CMM with rights acquired and included in the security module, rather than by intercepting the content itself. This is also made apparent by the examples of FIGs. 24-26. For example, with respect to FIG. 24, "[i]n stage 407, the SM decodes the CMMs, verifies that the time-shifting mode is authorized" (paragraph [0296]) then "[i]n stage 408, the HDVR module decrypts the control words, then sends them to the descrambler" (paragraph [0297]). The security nature of the content is determined in stage 407 before the content is descrambled following sending the control words to the descrambler in stage 408. Therefore, the security nature cannot be determined by intercepting the content because the content is not sent until after the security nature is known.

Claim 31 also requires "determining from the security information if the user has necessary access privilege in the operating system layer to access the encrypted data portion without consulting with another machine." Again, *Leporini* does not teach this limitation. For example, access privileges in *Leporini* are handled in the Device Interface level 256. The Device Interface layer 256 is a different layer from the System Software/Hardware layer 258 which is the operating system provided by the manufacturer of the receiver/decoder (paragraph [0191]). The Device Interface layer 256 includes devices such as card readers (paragraph [0190]). Examples of low level devices 4068 are LCARD and RCARD devices which enable communications with smartcards in smartcard readers 4036 (paragraph [0194]). As noted above, the CMPS is distributed across security modules (SM) on smartcards, for instance, the conditional access

smartcard 48 is identified with the CAS SM in paragraph [0339]. Thus, security information is determined by security modules at the level of devices in the Device Interface layer 256 and not at the operating system layer as required by claim 31.

Based at least upon the above remarks, Applicants submit that claim 31 is allowable in view of the combination of *Leporini* with *Pensak* and request that claim 31 be allowed. Furthermore, since claims 32-40 depend from claim 31, Applicants submit that claim 32-40 are also allowable for at least the same reasons given above in conjunction with claim 31.

In paragraph 37 of the Office Action, the Examiner rejected claims 6-9, 26, and 27 under 35 U.S.C. §103(a) as being unpatentable over the combination of *Leporini* and *Pensak* in further view of Ozog et al. (U.S. Pub. No. 2003/0033528, hereinafter *Ozog*). Applicants traverse the rejection.

Claims 6-9 depend from claim 1 and claims 26 and 27 depend from claim 20. As provided above, claims 1 and 20 are allowable over *Leporini* and *Pensak*. The addition of *Ozog* does not cure the deficiencies of *Leporini* and *Pensak*. As such, claims 6-9, 26, and 27 are allowable.

In paragraph 39, the Examiner rejected claims 41-88 as "they disclose the same invention as in claims 1-40 and do not further limit the claimed invention, therefore, they are rejected under the same rationale." Based upon at least the above remarks with respect to claims 1-40, Applicants submit that claims 41-88 are allowable in view of *Leporini* and *Pensak* with or without *Ozog*, and therefore request that claims 41-88 also be allowed.

CONCLUSION

Based on the foregoing remarks, Applicants believe that the rejections in the Office Action of December 21, 2005 are fully overcome, and that the Application is in condition for allowance. If the Examiner continues to reject the claims, Applicants request that the Examiner provide a detailed rebuttal to Applicants' arguments that would be sufficient for the Applicants to respond properly. Should the Examiner have questions regarding the case, the Examiner is invited to contact Applicants' undersigned representative at the number given below.

Respectfully submitted,
Alain Rossmann, et al.

Date: 6/19/06 By: Susan Yee

Susan Yee, Reg. No. 41,388
Carr & Ferrell LLP
2200 Geng Road
Palo Alto, CA 94303
Phone:(650) 812-3400
Fax: (650) 812-3444